ОТЗЫВ

на автореферат диссертации Березина Андрея Николаевича «Методы повышения уровня безопасности защитных преобразований информации», представленной к защите на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

В автореферате диссертации А.Н. Березина в достаточно полно раскрывается актуальность диссертационного исследования, ее цель и исследовательские задачи. Выполненная работа посвящена достаточно важному для практики информационной безопасности вопросу повышения уровня безопасности защитных преобразований информации. Автором разработан и обоснован новый метод реализации подхода к построению протоколов защитных преобразований информации, злом которых требует одновременного решения задачи факторизации и задачи дискретного логарифмирования в простом конечном поле. Предложенный в диссертации метод свободен от недостатков ранее известного метода аналогичного назначения и позволяет построить различные типы практичных протоколов, обладающих повышенным уровнем безопасности.

Новизна полученных результатов состоит в разработке нового метода построения алгоритмов и протоколов защитных преобразований информации указанного типа и разработке ряда новых протоколов, имеющих практическую значимость.

Судя по автореферату, диссертационная работа хорошо структурирована и представляет законченное научное исследование. Результаты, выносимые на защиту, прошли апробацию на конференциях различного уровня и достаточно полно опубликованы в 5 журналах, входящих в перечень ВАК.

К недостаткам стоит отнести следующие:

1) недостаточно полно освещены потенциально возможные атаки на разработанные протоколы;

2) некоторые из разработанных протоколов упомянуты в автореферате, но не описаны, например, протокол интерактивной аутентификации.

Указанные недостатки, видимо, связаны с ограниченностью объёма автореферата и принципиально не влияют на общую оценку диссертационной работы Березина А.Н., которая имеет существенную практическую и теоретическую значимость, отвечает п.9 «Положения о порядке присуждения учёных степеней» и соответствует требованиям ВАК к кандидатским диссертациям, а её автор, А.Н. Березин заслуживает присуждения учёной степени кандидата технических наук по специальности 05.13.19 - «Методы и системы защиты информации, информационная безопасность».

Профессор кафедры КОИБ, д.т.н. Гаскаров В.Д.

gaskarow@yandex.ru